IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Attwood et al.**	§	
	§	Group Art Unit: **2134**
Serial No. **09/503,608**	§	
	§	Examiner: **Tran, Ellen C.**
Filed: **February 11, 2000**	§	
	§	
For: **Technique of Defending Against Network Flooding Attacks Using a Connectionless Protocol**	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

36736
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

REPLY BRIEF (37 C.F.R. 41.41)

This Reply Brief is submitted in response to the Examiner's Answer mailed on July 18, 2007.

No fees are believed to be required to file a Reply Brief. If any fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0461.

RESPONSE TO EXAMINER'S ANSWER

The Examiner continues to make erroneous assertions in the Examiner's Answer. Therefore, this Reply Brief is necessary. Appellants reproduce claim 1 below for the convenience of the Board:

> 1. A method of preventing a flooding attack on a network server in which a large number of connectionless datagrams are received for queuing to a port on the network server, comprising:
>
> determining, in response to the arrival of a connectionless datagram from a host for a port on the network server, if the number of connectionless datagrams already queued to the port from the host exceeds a prescribed threshold;
>
> discarding the datagram, if the number of connectionless datagram already queued to the port from the host exceeds the prescribed threshold; and
>
> queuing the connectionless datagram to a queue slot of the port, if the number of connectionless datagram already queued to the port from the host does not exceed the prescribed threshold.

In the Examiner's Answer of July 18, 2007, the Examiner makes numerous incorrect assertions regarding the teachings of *Schuba*. The Examiner's mistaken assertions are based on a fundamental misunderstanding of the technological facts at issue. In particular, the Examiner incorrectly believes that a group of half-open connections, as taught in *Schuba*, is the same as a queue of connectionless datagrams, as recited in the claims.

The Examiner repeatedly makes this incorrect assertion. Rather than repetitiously address each statement made by the Examiner, Appellants elect to cut to the heart of the issue and rebut one set of representative statements made in the Examiner's Answer. In particular, the Examiner states that:

> The Examiner disagrees with applicant's interpretation, the Examiner reiterates the following points:
>
> - a half-open connection is a 'connectionless datagram
> - multiple half-open connections is a 'queue of connectionless datagrams'
> - Listening for incoming SYN packets and determining if a limit is reached is 'determining the number of connectionless datagrams', because a SYN packet is a connectionless datagram.

Examiner's Answer of July 18, 2007, p. 12.

Each assertion separated by a "-" is factually incorrect. Appellants address each assertion in turn.

The Examiner first asserts that a half-open connection is a "connectionless datagram." This assertion is plainly wrong. To assist the Board in understanding why the Examiner is plainly wrong, Appellants invite the Board to review an article, cited below, published on the Internet by CISCO systems. CISCO systems is one of the most established Internet technology companies on Earth, and is known for its technological expertise in this area. On the subject of denial of service attacks, the CISCO publication states the following:

> Bandwidth attacks-These DDoS attacks consume resources such as network bandwidth or equipment by overwhelming one or the other (or both) with a high volume of packets. Targeted routers, servers, and firewalls-all of which have limited processing resources-can be rendered unavailable to process valid transactions, and can fail under the load.
>
> The most common form of bandwidth attack is a packet-flooding attack, in which a large number of seemingly legitimate TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) packets are directed to a specific destination. To make detection even more difficult, such attacks might also spoof the source address-that is, misrepresent the IP address that supposedly generated the request to prevent identification.
>
> Application attacks-These DDoS attacks use the expected behavior of protocols such as TCP and HTTP to the attacker's advantage by tying up computational resources and preventing them from processing transactions or requests. HTTP half-open and HTTP error attacks are just a couple examples of application attacks.

http://www.cisco.com/en/US/netsol/ns615/networking_solutions_white_paper0900aecd8011e927.shtml

Thus, the CISCO systems publication makes a clear distinction between two different types of denial of service attacks: bandwidth flooding attacks and application attacks. In bandwidth flooding attacks, *a large number of packets* are directed towards an address in an attempt to overwhelm the physical capabilities associated with that address. In this case, a *queue of connectionless datagrams* accumulates. This problem is the problem addressed by claim 1, which specifically requires, "determining, in response to the arrival of a connectionless datagram

from a host for a port on the network server, *if the number of connectionless datagrams already queued to the port from the host exceeds a prescribed threshold*."

The Examiner appears to confuse the plain language of claim 1, which addresses bandwidth attacks, with the issue of application attacks. According to the CISCO systems publication, application attacks take advantage the expected behavior of protocols. In particular, application attacks prevent legitimate requests from being processed. One method of implementing an application attack is to create many HTTP half-open connections on the operating system of the host. If too many half-open connections arise, then the host operating system is no longer able to process requests. Although a half-open connection is created using a data packet, the half-open connection itself *does not accumulate a queue of connectionless datagrams*.

This half-open situation, which occurs during application attacks, is not addressed by claim 1. The plain language of claim 1 is directed towards queues of the connectionless diagrams.

To draw an analogy in a non-limiting example, the queue in claim 1 is similar to a line (or queue) of customers waiting to buy tickets at a booth. In this analogy, the booth is the port and each customer is a connectionless datagram.

Continuing with this analogy, a group of half-open connections corresponds to *a group of individual, single* "fake customers" at *each of many different ticket booths*. Each ticket booth thinks a real customer is about to make a purchase, because the booth has been told to expect input. However, the customer is a fake customer and so no such input arrives. Instead, the fake customer simply "stands in the way" of all of the other customers. Unfortunately, the booth cannot process any additional transactions because the expected input has not been received. Note that operating systems operate many ports. To continue the analogy, there are many ticket booths. As a result of individual, single fake customers standing at every available booth, *every available booth* becomes unavailable to legitimate customers.

Put more simply, claim 1 is directed towards discarding packets if too many packets accumulate at a gate. The Examiner's scenario, and that described in *Schuba*, is directed towards *a group of* gates being unavailable due to half-open connections. *Schuba* does not discard the packets that are accumulating at the gates; rather, *Schuba discards the gates themselves.* The

two situations are completely different. For this reason, *Schuba* does not teach the plain meaning of the explicit language of claim 1. Accordingly, under the standards of *In re Bond*, *Schuba* does not anticipate claim 1.

Additionally, the Board is invited to review the following article at Wikipedia.com, which is consistent with the above publication by CISCO systems:

> A **half-open connection** refers to a TCP connection that is partially open.
>
> The TCP protocol has a three state system for opening a connection. First, the originating site (A) sends a SYN packet to the destination (B). A is now half-open, and awaiting a response. B now updates its kernel information to indicate the incoming connection from A, and sends out a request to open a channel back (the SYN/ACK packet).
>
> At this point, B is now "half-open" (it has sufficient information to receive packets, but not enough to send packets back). Note that B was put into this state by another machine, outside of B's control.
>
> Under normal circumstances (see denial-of-service attack for deliberate failure cases), A will receive the SYN/ACK from B, update its tables (which now have enough information for A to both send and receive), and send a final ACK back to B.
>
> Once B receives this final ACK, it also has sufficient information for two-way communication, and the connection is fully open.

http://en.wikipedia.org/wiki/Half-open_connection (emphasis in original)

Again, half-open connections refer to the status of various gates of the operating system of a host. This state is entirely different than a queue of connectionless datagrams, as required by claim 1. Accordingly, under the standards of *In re Bond*, *Schuba* does not anticipate claim 1. For similar reasons, all of the other arguments made by the Examiner collapse.

Appellants next address the Examiner's assertion that, "multiple half-open connections is a 'queue of connectionless datagrams.'" In view of the analysis and facts presented above, this assertion is also plainly wrong. Multiple half-open connections are just that - multiple half-open connections at multiple corresponding kernel ports. A queue of connectionless datagrams is also just that - a line of packets waiting to be processed at a single port, whether that port is physical (as in a router) or is embodied by software (as in a kernel of an operating system). The former is a group of half-open connections, not a queue. The latter is a queue.

Appellants next address the Examiner's assertion that, "Listening for incoming SYN packets and determining if a limit is reached is 'determining the number of connectionless datagrams', because a SYN packet is a connectionless datagram." Again, the Examiner's assertion is confused because the Examiner is confused as to the difference between the different types of denial of service attacks. "Listening for incoming SYN packets and determining if a limit is reached" is not "determining a number of connectionless" because the "limit" referred to by the Examiner relates to the number of half-open connections and not to the number of connectionless datagrams at each port.

Additionally, Appellants point out that an important difference exists between "determining a number of connectionless datagrams" and "determining if a limit is reached." The number of connectionless datagrams can be, and almost always is, different than a limit. Thus, the Examiner has no basis to assert that "determining if a limit is reached" is the same as "determining a number."

Because the Examiner's assertions are plainly wrong, nothing in *Schuba* is equivalent to the claimed features at issue. Accordingly, under the standards of *In re Bond*, *Schuba* does not anticipate claim 1. For similar reasons, all of the other rejections collapse.

CONCLUSION

As shown above, the Examiner's assertions regarding the teachings of *Schuba* are manifestly incorrect. All of the rejections rely on the Examiner's assertions regarding *Schuba*. Therefore, all of the rejections are erroneous. Accordingly, Appellants request that the Board of Patent Appeals and Interferences reverse the rejections. Additionally, Appellants request that the Board direct the Examiner to allow the claims.

/Theodore D. Fay III/
Theodore D. Fay III
Reg. No. 48,504
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777